PACIFIC JOURNAL OF MATHEMATICS
Vol. 43, No. 1, 1972

THE DIOPHANTINE PROBLEM $Y^2 - X^3 = A$ IN A POLYNOMIAL RING

DENNIS L. JOHNSON

Let $C[z]$ be the ring of polynomials in z with complex coefficients; we consider the equation $Y^2 - X^3 = A$, with $A \in C[z]$ given, and seek solutions of this with $X, Y \in C[z]$ i.e. we treat the equation as a "polynomial diophantine" problem. We show that when A is of degree 5 or 6 and has no multiple roots, then there are exactly 240 solutions (X, Y) to the problem with $\deg X \leqq 2$ and $\deg Y \leqq 3$.

It is possible that, A being of degree 6, solutions (X, Y) exist with $\deg X > 2$ or $\deg Y > 3$. We "normalize" the problem so as to remove these from our consideration, and give the following definitions: if A is any polynomial of degree d, we shall permit its *formal degree* to be any integer *divisible by* 6 and greater or equal to d. Given A of formal degree $6k$, we require the solutions X, Y of the equation to be of formal degrees $2k$, $3k$ resp., i.e. $\deg X \leqq 2k$, $\deg Y \leqq 3k$. This problem will be called the *problem of order* k. The restriction on the degrees of X, Y causes no loss in generality, for if k is chosen large enough, it will exceed $1/2 \deg X$ and $1/3 \deg Y$. Furthermore, the classification by k has a natural geometric interpretation. We confine our attention to the problem of order 1. The order restriction enables us to projectivize the equation to an equation of degree $6k$, with $\deg A = 6k$, $\deg X = 2k$, $\deg Y = 3k$.

Suppose then that A has formal degree 6, and (X, Y) is a solution of proper formal degree, $\deg X \leqq 2$, $\deg Y \leqq 3$. The projective curve K: $w^3 - 3Xw + 2Y = 0$ has the z-discriminant $Y^2 - X^3 = A$, so the function $z: K \to S^2$ (proj. line) has its branches among the roots of A, for finite z. At $z = \infty$ we introduce $\tilde{z} = 1/z$, $\tilde{w} = w/z = \tilde{z}w$ and get

$$\tilde{z}^3 w^3 - 3\tilde{z}^3 X\left(\frac{1}{\tilde{z}}\right)w + 2\tilde{z}^3 Y\left(\frac{1}{\tilde{z}}\right) = 0 :$$

If $X = a_0 z^2 + \cdots$, $Y = b_0 z^3 + \cdots$, then

$$F = \tilde{w}^3 - 3(a_0 + a_1\tilde{z} + a_2\tilde{z}^2)\tilde{w} + 2(b_0 + b_1\tilde{z} + \cdots) = 0$$

and

$$\frac{\partial F}{\partial \tilde{w}} 3\tilde{w}^2 - 3(a_0 + \cdots) .$$

Now at $\tilde{z} = 0$ (i.e. $z = \infty$) z has a branch point if and only if $\partial F/\partial \tilde{w} = 0$;

i.e. we must have

$$\tilde{w}^3 - 3a_0\tilde{w} + 2b_0 = 0$$

and

$$3\tilde{w}^2 - 3a_0 = 0$$

which is true if and only if $\Delta = -a_0^3 + b_0^2 = 0$ i.e. if and only if $\deg A < 6$. Hence if $\deg A < 6$, we put a "formal root" of A at ∞ with multiplicity 6-$\deg A$.

We now assume the roots of A to be *distinct*. This entails $\deg A = 5$ or 6, with no multiple (finite) roots. The roots will be called $z_1, \cdots, z_6$. Note that if either X or Y were zero at z_ι, the other would also be, since A is zero there (for the case $z_\iota = \infty$ just imagine the projective form of $Y^2 - X^3 = A$; the statement then reads that $\deg A < 6$ and if $\deg Y < 3$ then $\deg X < 2$ and conversely). Hence A would have at least a *double* zero at z_ι, (or at ∞: $\deg A \leqq 4$) contrary to hypothesis. Hence $X, Y \neq 0$ at z_ι, and $\deg X = 2$ or $\deg Y = 3$. Away from a branch point we may write locally:

$$w_0 = \sqrt[3]{-Y + \sqrt{A}} + \sqrt[3]{-Y - \sqrt{A}}$$

$$w_1 = \omega\sqrt[3]{-Y + \sqrt{A}} + \omega^2\sqrt[3]{-Y - \sqrt{A}}$$

$$w_2 = \omega^2\sqrt[3]{-Y + \sqrt{A}} + \omega\sqrt[3]{-Y - \sqrt{A}}$$

for proper choice of the roots; as we go around z_ι, $\sqrt{A}$ changes to $-\sqrt{A}$, and we get a root permutation $w_0 \leftrightarrow w_0$, $w_1 \leftrightarrow w_2$. Thus the branching number b_ι at z_ι is 1, and the total branching is 6, so the genus is $g = b/2 - r + 1 = 1$, i.e. K is a torus.

We should also prove that K is irreducible; but if K were reducible, factoring as $(w - \alpha)(w^2 + \alpha w + \beta)$ (where α, β are polynomials in z by Gauss's lemma) i.e., we have $3X = \alpha^2 - \beta$ and $2Y = -\alpha\beta$, and $A = Y^2 - X^3 = 4\beta^3 + 15\alpha^2\beta^2 + 12\alpha^4\beta - 4\alpha^6 = -(\alpha^2 - 4\beta)(2\alpha^2 + \beta)^2$. It is easy to see that $\deg \alpha \leqq 1$, $\deg \beta \leqq 2$, and hence $\deg(\alpha^2 - 4\beta) \leqq 2$. Since $\deg A \geqq 5$ we see that $\deg(2\alpha^2 + \beta) \geqq 1$, whence A has double roots, contrary to hypothesis.

Thus, any solution X, Y gives us an elliptic curve K represented as a 3-sheeted branched covering of S^2 with branch points at z_ι, where $z: K \rightarrow S^2$ is an elliptic function of degree 3. Furthermore, w is also a function on K, and its poles are among those of z, and of order $\leqq$ the order of the z-poles: for expanding w_ι at $z = \infty$ we get

$$w_\iota = \omega^\iota\sqrt[3]{-b_0z^3 + \cdots + \sqrt{(b_0^2 - a_0^3)z^6 + \cdots}} + \omega^{2\iota}\sqrt[3]{\text{etc.}}$$

i.e.

$$w_\iota = \left(\omega^\iota \sqrt[3]{-b_0+\sqrt{\Delta}} + \omega^{2\iota}\sqrt[3]{-b_0-\sqrt{\Delta}}\right)z + \text{lower powers of } z$$

i.e. the order of w is $\leqq$ order of z at all places $z=\infty$. (Clearly w has no other poles). Note also that the sum Σw_ι of the three values of w over any z is zero.

Now suppose conversely that we are given a branched covering of S^2 with 6 simple branch points at the roots of A; we then have an elliptic curve K and a meromorphic function z: $K \rightarrow S^2$ with 3 poles (one of which is double if a branch point is at ∞) at places k_1, k_2, k_3. Now the set of meromorphic functions w on K whose poles are among the k_ι form a vector space V of dimension 3. Given any such w, the sum $w_0+w_1+w_2$ of its 3 values over any z gives us a function which is:

(1) finite for finite z

(2) of order $\leqq$ the order of z at $z=\infty$

(3) symmetric in the sheets, so rational in z.

Hence Σw_ι must be *linear* in z: $\Sigma w_\iota = a_w z + b_w$, where a_w and b_w are constants depending on w. Note that a_w and b_w are clearly *complex-linear* in w, i.e. a, b: $V \rightarrow C$ are linear maps. Furthermore, since both $w=1$ and $w=z$ are in V we have a and b are linearly independent: for

$$a(1)=0 \qquad a(z)=3$$

$$b(1)=3 \qquad b(z)=0$$

and so $a_w=0$, $b_w=0$ defines a one dimensional subspace of V i.e. a $w\neq 0$, defined up to a constant multiple, of degree $\leqq 3$, with its poles among those of z, and with $\Sigma w_\iota = 0$. Hence w satisfies some equation

$$w^3 - 3Pw + 2Q = 0, \text{ with } P \;\&\; Q \text{ rational in } z\,;$$

but

$$-3P = w_1w_2 + w_2w_3 + w_3w_1 \text{ is } \textit{finite} \text{ for } z \text{ finite}\,;$$

hence P is a polynomial; also its degree is $\leqq 2$ since the order of w_ι is $\leqq$ that of z at ∞. Likewise Q is a polynomial of degree $\leqq 3$ in z. Finally w is not rational in z since if it were, it would actually be linear, $w=az+b$, and then

$$\Sigma w_\iota = 3w = 3az+3b = 0, \quad \text{i.e.} \quad w\equiv 0\,.$$

Hence $w^3-3Pw+2Q=0$ is irreducible, and thus *defines* the curve K. Because of this, we must have the branch points as roots of the discriminant $Q^2 - P^3$ $(\neq 0)$; i.e. $A \mid Q^2 - P^3$; $\deg Q^2 - P^3 \leqq 6$, and is <6 if and only if as we have seen previously, ∞ is a branch point of K; in the latter case we also have $\deg A = 5$, and so in every case we have $\deg(Q^2 - P^3) = \deg A$, i.e. $A = k(Q^2 - P^3)$ for some constant $k \neq 0$. If now we replace w by $w/\alpha (\alpha \in C)$, we replace P by P/α^2 and Q by Q/α^3 and $Q^2 - P^3$ by $(Q^2 - P^3)/\alpha^6$; Hence we may choose a scale factor α, determined up to a 6th root of unity, and a rescaled w such that $Q^2 - P^3 = A$, i.e. (P, Q) is a solution. Thus we have shown that any 3 sheeted covering of S^2 with simple branches at $A = 0$ gives us exactly 6 solutions to the problem (These 6 solutions are distinct since two could be equal if and only if P or $Q \equiv 0$, which is impossible). Furthermore, if we have two different such branched coverings K_1, K_2, then the corresponding solutions (P_1, Q_1), (P_2, Q_2) must be distinct, since the data (P_ι, Q_ι) actually *define* K.

Thus the only remaining problem is to enumerate the different coverings possible.

We choose a base point $q \in S^2$, distinct from the roots z_ι, and loops p_ι $(\iota = 1, \cdots, 6)$ encircling the roots z_ι acting as free generators of the fundamental group $\pi_1(S^2 - \bigcup_j z_j)$, subject only to the relation $p_1 \cdots p_6 =$ identity. Choosing a numbering 1, 2, 3 of the sheets over q, each p_ι determines a permutation π_ι (in S_3) of the sheets, and these completely determine the surface. Since the branches are all simple, these permutations must be *transpositions*: (12), (23) or (31). Also not all the π_ι can be equal, for then two sheets over q would remain unconnected from the third. If we choose $\pi_1, \cdots \pi_5$ arbitrarily then π_6 is determined by $\pi_1 \pi_2 \cdots \pi_6 = e$. Note however that $\pi_1, \cdots \pi_5$ may not be chosen all equal, since π_6 would also be same by virtue of the relation. Hence we may choose $\pi_1, \cdots \pi_5$ in $3^5 - 3$ ways, obtaining all possible coverings of the required nature. Two such choices π_ι, π'_ι give the same covering if and only if they differ by a renumbering of the sheets over q, i.e. if and only if $\pi'_\iota = g\pi_\iota g^{-1}$ for some $g \in S_3$. Since at least two different transpositions occur among the π_ι, conjugation by the elements of S_3 produces exactly 6 different equivalent choices of π_ι; hence the total number of different surfaces is $(3^5 - 3)/6 = (3^4 - 1)/2 = 40$. Remembering that to each such surface there are 6 solutions, we have:

THEOREM. *If A is a polynomial of degree* 5 *or* 6 *without multiple roots, then there are exactly* 240 *distinct solutions of the equation $Y^2 - X^3 = A$ in polynomials X, Y for which* $\deg X \leqq 2$, $\deg Y \leqq 3$.

It should be pointed out that, in principle at least, the determination of the solutions (X, Y) for a given A could be solved by classical elimination theory. For example, if $X = a_0 z^2 + a_1 z + a_2$ and

$Y = b_0z^3 + b_1z^2 + b_2z + b_3$ is a solution to $Y^2 - X^3 = A = \alpha_0z^6 + \cdots + \alpha_6$, then treating the a_ι and b_j as unknowns, formal manipulation and the equating of coefficients gives us 7 polynomial equations in 7 unknowns which presumably (assuming independence) gives a finite set of solutions for the unknowns a_ι, b_j. This also shows us that the a_ι and b_j are algebraic over the field of the α_k. In practice, however, this elimination would probably not be computationally feasible.

Received July 15, 1971. This paper presents the results of one phase of research carried out at the Jet Propulsion Laboratory, California Institute of Technology, under Contract No. NAS 7-100, sponsored by the National Aeronautics and Space Administration.

JET PROPULSION LABORATORY
CALIFORNIA INSTITUTE OF TECHNOLOGY